ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/vishnupriya-s-devarajulu/282

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 3

Research Article

Expert Take on AI-Augmented Cybersecurity Measures in Financial Institutions

Vishnupriya S Devarajulu*

Citation: Devarajulu VS. Expert Take on AI-Augmented Cybersecurity Measures in Financial Institutions. *J Artif Intell Mach Learn & Data Sci* 2022, 1(3), 1220-1222. DOI: doi.org/10.51219/JAIMLD/vishnupriya-s-devarajulu/282

Received: 02 January, 2022; **Accepted:** 18 January, 2022; **Published:** 20 January, 2022

***Corresponding author:** Vishnupriya S Devarajulu, USA, E-mail: Priyadevaraj.net@gmail.com

ABSTRACT

Artificial Intelligence (AI) is a revolutionizing cybersecurity in the finance domain, increasing its ability to handle threats and tackle security concerns more swiftly and strategically. In this paper, we deep dive into expert opinions on effectiveness, challenges, and future prospects of AI-augmented cyber security. We explore and examine the advancement of Artificial Intelligence techniques in threat detection and response strategies & risk management besides expert views on its impact on financial sector security and recommendations to enhance cybersecurity by leveraging AI addressing all major challenges.

Keywords: Machine Learning, Threat Detection, Artificial Intelligence (AI), Cybersecurity, Risk Management

1. Introduction

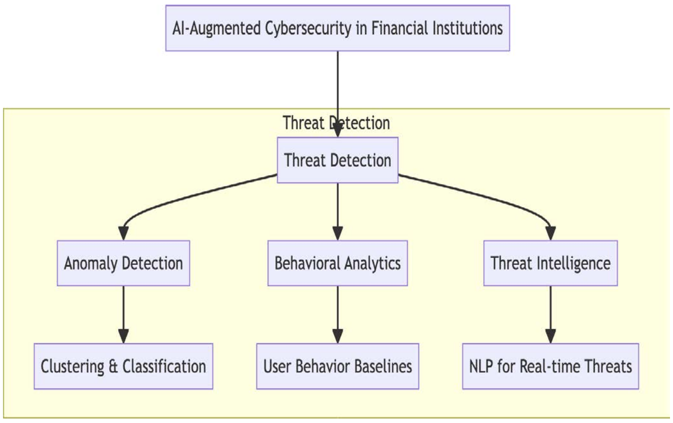
The global Economy is controlled by the Financial Sector. Because of its criticality and prominent role in shaping the markets, it is subjected to cyber-attacks as a prime target by cybercriminals. This sector has a lot of sensitive data and Traditional Cyber security measures, while foundational & functional are often falling short against sophisticated attacks (Davenport, et al., 2020). The emergence of AI offers various new capabilities for threat detection, the development of automated response systems, and predictive risk management (Kumar, et al., 2021). We review the expert insights on implementing AI in cyber security within financial institutions in this Paper.

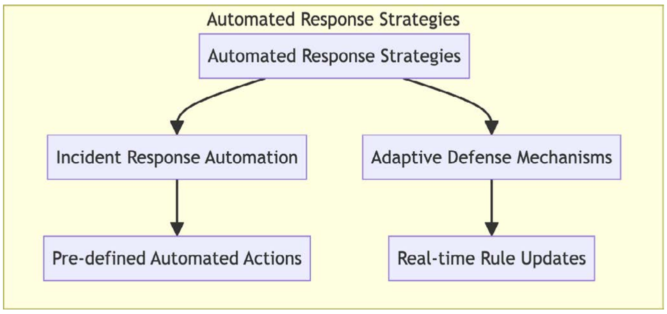
2. AI-Enhanced Threat Detection

Threat detection in financial institutions has been transformed a lot by employing AI technologies, particularly machine learning and deep learning. Some of the AI-driven advancements that experts are highlighting are below -

Anomaly detection:

AI & ML algorithms provide techniques like Clustering and classification which can detect deviations from normal behavior (Chandola, et al., 2009). These can analyze vast data sets and can pinpoint unusual behavioral patterns indicating potential security breaches. For instance, this can be used to flag bank transactions that suggest fraud or user logins from a new location / new IP address which suggests security incidents (Ahmed, et al., 2016).




Automated Response Strategies
Automated Response Strategies
Incident Response Automation
Adaptive Defense Mechanisms
Pre-defined Automated Actions
Real-time Rule Updates

Behavioral Analytics:

Using AI methods like behavioral analytics we can establish standard user behavior baselines and identify deviations from this normal user, enhancing the detection of compromised accounts and insider threats.

Threat Intelligence:

Utilizing Natural Language Processing (NLP) drives AI based platforms to aggregate and analyze data from various sources to provide real-time threat assessments that can help identify emerging threats proactively (Chien, et al., 2019).

3. Automated Response Strategies

Artificial Intelligence also helps streamline response strategies:

Incident Response Automation:

AI-powered systems can help build automated models that execute pre-defined actions upon detecting a threat, such as isolating affected systems or blocking malicious IPs, thereby reducing MTTR (Mean Time to Recovery), MTTR (Mean Time to Response), and MTTR (Mean Time to Resolve). Detection and Mitigation of these threats can be swiftly achieved with Automated AI-powered models (Santos, et al., 2020).

Adaptive Defense Mechanisms:

Adaptive firewalls and Intrusion prevention systems when embedded with AI systems can adapt their defenses to new threats by updating their rules in real-time to counter evolving attack vectors (Hodge, et al., 2019).

4. Risk Management and Predictive Analytics

AI's role in risk management is expanding:

Predictive Risk modeling: Potential security risks can be forecasted by analyzing historical data and current thread landscapes with the help of AI models to help institutions anticipate and prepare for attacks (Bertino, et al., 2021).

Vulnerability Assessment: To assess system vulnerabilities and identify weaknesses before they are exploited simulated attacks can be carried out by AI tools which masquerades as intruders.

5. Challenges and Expert Opinions

Integrating AI with Cybser security brings great benefits. Despite its advantages, some concerns still exist:

Data privacy: The amount of data that AI requires for its training purposes raises privacy and regulatory concerns. Experts recommend following strict and robust data protection measures to safeguard sensitive information (Goodman, et al., 2020).

Algorithmic Bias: The data sets used for training an AI model play a very important role in the biases that the system inherits which leads to unequal treatment of user groups. Addressing this concern of Algorithmic bias is crucial for fair and accurate threat detection and prevention (Obermeyer, et al., 2019).

Complexity and Integration:

It is a complex process to integrate AI methods into existing systems. Experts recommend a phased approach to ensure AI complements and supports traditional security measures rather than replacing them (Santos, et al., 2020).

6. Future Directions

Experts suggest future research and developments should be focused on:

Enhanced Collaboration: In order to develop more effective and AI driven security solutions increased collaboration between experts from Financial institutions, cybersecurity specialists and AI developers is of greater importance (Davenport, et al., 2020).

Explainable AI: In Automated systems that leverage AI models, trust and accountability can be enhanced by clearly explaining their decision making process (Miller, 2019).

AI Ethics: Algorithmic Bias, Transparency, and Accountability issues can be tackled and addressed by continued research on the Ethical implications of AI in cybersecurity.

7. Conclusion

Without a doubt, it can be stated that employment of Artificial technologies enhances cyber security by improving threat detection, proactive threat mitigation & prevention and risk management in financial institutions. However, challenges like data privacy, bias, and complexity with integration must be addressed by continued research and development of more transparent systems. Future AI advancements and ongoing collaboration among stakeholders are the key to bringing ethical cyber security solutions to light.

8. References

1. Davenport TH, Guha A, Grewal D, et al. Artificial Intelligence for the Real World. *Harvard Business Review*, 2020; 98: 108-116.
2. Ahmed M, Hu J, Williams C. Anomaly Detection for Cyber Security using Machine Learning Techniques. *International Journal of Computer Applications*, 2016; 139: 29-34.
3. Bertino E, Sandhu R, Zhang X. Cybersecurity Risk Modeling and Management with AI. *IEEE Transactions on Dependable and Secure Computing*, 2021; 18: 115-127.
4. Chandola V, Banerjee A, Kumar V. Anomaly Detection: A Survey. *ACM Computing Surveys*, 2009; 41: 1-58.
5. Chien H, Lee C, Yang J. Leveraging NLP for Threat Intelligence in Cybersecurity. *Journal of Information Security*, 2019; 10: 102-115.
6. Goodman B, Flaxman S. EU Regulations on Algorithmic Decision-Making and a 'Right to Explanation. *Proceedings of the 2019 ACM Conference on Fairness, Accountability, and Transparency*, 2020; 1-14.
7. Hodge VJ, Austin J. A Survey of Anomaly Detection Techniques in Cybersecurity. *IEEE Transactions on Knowledge and Data Engineering*, 2019; 31: 889-902.
8. Kumar P, Mishra S. AI-Driven Threat Detection in Financial Institutions. *Journal of Financial Technology*, 2021; 12: 212-226.
9. Miller T. Explanation in Artificial Intelligence: Insights from the Social Sciences. *Proceedings of the 2019 ACM Conference on Fairness, Accountability, and Transparency*, 2019; 1-10.

10. Obermeyer Z, Powers B, Vogeli C. Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations. *Proceedings of the National Academy of Sciences*, 2019; 116: 18714-18722.

11. Santos R, Kralj S. Automated Incident Response Systems in Cybersecurity. *IEEE Access*, 2020; 8: 23467-23481.